REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
28-11-2009	Final Report	15-Apr-2007 - 14-Apr-2008

4. TITLE AND SUBTITLE

Sequence Design for Secure and Reliable Communications Networks

5a. CONTRACT NUMBER
W911NF-07-1-0148

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS
John Q. Liu

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Wayne State University
Sponsored Program Administration
5057 Woodward, Suite 6402
Detroit, MI 48202 -

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
52588-CS.1

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
Sequences are critical in spread spectrum communications for anti-jamming and security. The complexity to break sequence is measured using linear span of sequence. The linear span of a sequence is the lowest degree of the characteristic polynomials that can generate the sequence. A new family of sequences with optimal correlation properties is constructed for the generalized Kasami set. A lower bound on the linear span is established. It is proved that with suitable choices of parameters, this family has exponentially larger linear spans than either No

15. SUBJECT TERMS
Sequence design, complexity, linear span, optimal correlation, ideal autocorrelation

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			John Liu
UU	UU	UU	UU		19b. TELEPHONE NUMBER: 313-577-3530

On The Linear Span of A Binary Sequence Family with Optimal Correlation Properties

ARO Grant W911NF-07-1-0148
Final Report

John Q. Liu
Wayne State University
Detroit, MI 48202

Abstract

Sequences are critical for anti-jamming and security in spread spectrum communications networks. The complexity to break sequence is measured by linear span of sequence. The linear span of a sequence is the lowest degree of the characteristic polynomials that can generate the sequence. A new family of sequences with optimal correlation properties is constructed for the generalized Kasami set. A lower bound on the linear span is established. It is proved that with suitable choices of parameters, the linear span of this family is exponentially larger than that of either No sequences or TN sequences. A class of sequences with ideal autocorrelation is also proved to have large linear span. Therefore, the new family of sequences can be employed by future spread spectrum networks to have better security and lower bit error rate in the presence of jamming.

Contents

List of Tables

1 Introduction

Families of binary sequences have served in practical CDMA systems, spread spectrum systems, and broadband satellite communications [1]. It is desired that they have low autocorrelation, low cross-correlation, and large linear span [2]. The Gold pairs [3], [4] and bent function sequences [5] as well as the Kasami sequences [6]-[8] have desirable correlation properties. However, these sequences have small values of linear span, except the bent function sequences. The family of binary sequences [9] can also achieve large linear span, but their correlation property or family size is inferior to that of Gold pairs and the Kasami sequences

The linear span of a sequence is the lowest degree of the characteristic polynomials that can generate the sequence. It is also called the linear complexity. A characteristic polynomial $f(x) = x^n - c_{n-1}x^{n-1} - \cdots - c_1 x - c_0$ generates a sequence $\{s(t)\}$, if there exists the recursive relation

$$\begin{aligned} s(k+n) &= c_{n-1}s(k+n-1) \\ &\quad + \cdots + c_1 s(k+1) + c_0 s(k),\ k = 0, 1, \cdots. \end{aligned} \tag{1}$$

In implementation, $x^n f(1/x)$ is the feedback polynomial of a linear feedback shift register that generates the sequence $\{s(t)\}$. Applying the Berlekamp-Massey algorithm [10], a sequence of the linear span l can be reconstructed from a portion of its length equal to $2l$. In other words, the complexity to reconstruct or break a linear spreading sequence is a linear function of its linear span. Therefore, communication systems prefer to have sequences of very large linear span.

The generalized Kasami signal set [11] and the small set of Kasami sequences [6] have the same optimal correlation properties. From the viewpoint of the interleaved sequences, the construction of the generalized Kasami signal set uses ideal autocorrelation sequences as its component sequences [11]. When the component sequences have large linear span, the constructed sequences are expected to have large linear span.

Let $tr_m^n(\cdot)$ denote the trace function from the finite field F_{2^n} to its subfield F_{2^m}. Define a class of binary sequences with period $2^n - 1$ as

$$\begin{aligned} &s_h(t) \\ &= tr_1^m\{\{tr_m^{mk}[(tr_{mk}^n(\alpha^{2t}) + \gamma_h \alpha^{(2^{mk}+1)t})^u]\}^r\} \end{aligned} \tag{2}$$

where $n = 2mk$, $r = 2^{m-1} - 1, u = 1 + 2^m + \cdots + 2^{(k-2)m}$ with $\gcd(u, 2^{mk} - 1) = 1$, $\gamma_h \in F_{2^{mk}}$. This family of sequences is a novel subfamily of the generalized Kasami signal set in [11].

This paper studies the linear span for the sequence family in Eq. (2). Section 2 gives necessary notations and preliminaries. Section 3 derives lower bounds on the linear span of the sequences. It is proved that for k as its optimal values $3 \le k \le 5$, a majority of sequences in the family of Eq. (2) have linear spans at least $O(n \cdot 2^{\frac{2n}{3}})$, which is exponentially larger than the linear span of either the No sequences [12] or the TN sequences [13]. Section 4 shows that a class of sequences with ideal autocorrelation property also has large linear span. Section 5 concludes the study.

2 Preliminaries

Let $\mathcal{F}$ be the family of M binary $\{0,1\}$ sequences of period $N = 2^n - 1$ given by

$$\mathcal{F} = \{\{s_h(t),\, 0 \le t \le N-1\} \mid 0 \le h \le M-1\}. \tag{3}$$

The *cross correlation function* of the sequences $\{s_h(t)\}$ and $\{s_l(t)\}$ in $\mathcal{F}$ is

$$R_{h,l}(\tau) = \sum_{t=0}^{N-1} (-1)^{s_h(t) - s_l(t+\tau)} \tag{4}$$

where $0 \le h, l \le M-1$, $0 \le \tau \le N-1$, and $t+\tau$ is computed modulo N. The *maximum magnitude* $R_{\max}$ of the correlation values is

$$R_{\max} = \max |R_{h,l}(\tau)| \tag{5}$$

where $0 \le h, l \le M-1$, $0 \le \tau \le N-1$, and the cases of in-phase autocorrelations ($h = l$ and $\tau = 0$) are excluded. A family of binary sequences of period $2^n - 1$ is said to have *optimal correlation property* if $R_{\max} \le 2^{\frac{n}{2}} + 1$. For $h = l$, $R_{h,l}(\tau)$, abbreviated by $R_h(\tau)$, is the *autocorrelation function* of $\{s_h(t)\}$. The sequence $\{s_h(t)\}$ is said to have an *ideal autocorrelation property* if

$$R_h(\tau) = \begin{cases} N & \text{if } \tau \equiv 0 \bmod N; \\ -1 & \text{otherwise.} \end{cases} \tag{6}$$

Let F_{2^n} be the finite field with 2^n elements, and $n = em$ for some positive integers e and m. The *trace function* $tr_m^n(\cdot)$ from F_{2^n} to F_{2^m} is defined by

$$tr_m^n(x) = \sum_{i=0}^{e-1} x^{2^{im}} \tag{7}$$

where x is an element in F_{2^n}.

The trace function has the following properties [14]:

i) $tr_m^n(ax + by) = a \cdot tr_m^n(x) + b \cdot tr_m^n(y)$, for all a, $b \in F_{2^m}$, x, $y \in F_{2^n}$.

ii) $tr_m^n(x^{2^m}) = tr_m^n(x)$, for all $x \in F_{2^n}$.

iii) $tr_1^n(x) = tr_1^m(tr_m^n(x))$, for all $x \in F_{2^n}$.

The operation of multiplying by 2 divides the integers modulo $2^m - 1$ into sets called the *cyclotomic cosets* modulo $2^m - 1$ [15]. The cyclotomic coset containing s is $\{s,\, 2s,\, 2^2 s,\, \cdots,\, 2^{e_s - 1} s\}$, where e_s is the smallest positive integer such that $2^{e_s} s \equiv s \pmod{2^m - 1}$. Furthermore, e_s divides m, and $e_s = m$ for m prime and $s \not\equiv 0 \pmod{2^m - 1}$. The smallest positive integer in the cyclotomic coset $\{s, 2s, 2^2 s, \cdots, 2^{e_s - 1} s\}$ is called the *coset leader* [15].

For two integers a and b with $a \le b$, let $[a, b]$ be the interval consisting of all integer c with $a \le c \le b$, and the *length* is $b - a + 1$. When $a = b$, $[a, b]$ is called a *single*

point interval and written as $[a]$. Two intervals $[a, b]$ and $[c, d]$ are *un-incorporative* if $b+2 \leq c$ or $d+2 \leq a$. A set of several pairwisely un-incorporative non-negative intervals $\{[a_j, b_j] \,|\, j \in J\}$ determines a positive integer $\sum_{j \in J} \sum_{x \in [a_j, b_j]} 2^x$, where J is an index set. For a positive integer c, there exists an index set K consisting of non-negative integers such that $c = \sum_{k \in K} 2^k$, which determines a set of un-incorporative intervals $\{[a_j, b_j] \,|\, j \in J\}$ such that $\bigcup_{j \in J} [a_j, b_j] = K$. This fact will be used in derivation of the main result in this paper.

The following notations are used in the rest of this paper:

- m, k, and n: positive integers, $n = 2mk$;
- F_{2^n}: the finite field with 2^n elements;
- α: a primitive element of F_{2^n};
- $\Gamma(m)$: the set consisting of all non-zero coset leaders modulo $2^m - 1$;
- $C_i = \{i2^j \pmod{2^m - 1} \,|\, j = 0, 1, \cdots, m-1\}$, i.e., the cyclotomic coset modulo $2^m - 1$ containing the element i;
- $e_i = |C_i|$;
- Z_p: a residue ring of integers modulo p;
- $V = \{0, 1, \cdots, k-1\}$, where k is a positive integer;
- $V^t = V \times V \times \cdots \times V$ is the Cartesian product of t copies of V;
- $w(i)$: the weight of integer i, i.e., the number of ones in the coefficients of the binary expansion of i;
- $\lfloor z \rfloor$: the largest integer not exceeding z;
- $[a, b]$: the integer interval consisting of all integers c with $a \leq c \leq b$.
- $\gamma_0 = 0, \gamma_1, \cdots, \gamma_{2^{mk}-1}$: all 2^{mk} elements of the field $F_{2^{mk}}$.

Define a family

$$\mathcal{F} = \{\{s_h(t)\}_{0 \leq t < 2^n - 1} \,|\, 0 \leq h \leq 2^{mk} - 1\} \tag{8}$$

of 2^{mk} binary sequences of period $N = 2^n - 1$, where

$$\begin{aligned} & s_h(t) \\ &= tr_1^m\{\{tr_m^{mk}[(tr_{mk}^n(\alpha^{2t}) + \gamma_h \alpha^{(2^{mk}+1)t})^u]\}^r\} \end{aligned} \tag{9}$$

and integers $1 \leq u \leq 2^{mk} - 1$, $1 \leq r \leq 2^m - 1$ are relatively prime to $2^{mk} - 1$, $2^m - 1$, respectively.

Since $tr_1^m\{[tr_m^{mk}(\beta^{ut})]^r\}$ is a sequence with ideal autocorrelation for a primitive element β in $F_{2^{mk}}$, $\mathcal{F}$ is a set of sequence with optimal correlation, i.e., satisfying the Welch bound [16]. Furthermore, $R_{h,k}(\tau) \in \{-1, 2^{\frac{n}{2}} - 1, -2^{\frac{n}{2}} - 1\}$ for any out-of-phase shift (h, k, τ) ($h \neq k$ or $\tau \neq 0$).

The paper provides a lower bound on the linear span of the family $\mathcal{F}$ with the parameters $r = 2^{m-1} - 1$ and $u = 1 + 2^m + \cdots + 2^{(k-2)m}$. In Section 3, we will consider a general case where

$$\begin{aligned} & s_h(t) \\ &= \textstyle\sum_{i \in I}\{tr_m^{mk}[(tr_{mk}^n(\alpha^{2t}) + \gamma_h \alpha^{(2^{mk}+1)t})^u]\}^i \end{aligned} \tag{10}$$

where $I \subseteq \{1, 2, \cdots, 2^m - 2\}$ is the index set such that the sequence

$$\sum_{i \in I}[tr_m^{mk}(\beta^{ut})]^i \tag{11}$$

has ideal autocorrelation property and $r = 2^{m-1} - 1 \in I$. A lower bound of the linear span for the general case is analyzed. When $I = C_r$, the sequence in Eq. (10) is the same as that in Eq. (9). Thus, the lower bound on the linear span of the family $\mathcal{F}$ is obtained.

3 Linear span of sequences

This section proves that sequences in the family $\mathcal{F}$ have large linear span. Key [17] described a method for determining the linear span of a binary sequence with period $2^n - 1$. The linear span of $\{s_h(t)\}_{0 \leq t < 2^n - 1}$, denoted by $LS(\{s_h(t)\})$, can be determined by expanding the expression of $s_h(t)$ as a polynomial in α^t of degree less than $2^n - 1$ and then counting the number of monomials in α^t with nonzero coefficients occurring in the expansion. This technique will be applied to determine the linear span of sequences in family $\mathcal{F}$.

Denote each exponent $i \in I$ in Eq. (10) as

$$i = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_{w(i)}} \tag{12}$$

where $0 \leq i_1 < i_2 < \cdots < i_{w(i)} \leq m - 1$.

Let $x = \alpha^t$ and $y = x^{2^{mk}-1}$. Substituting Eq. (12) into Eq. (10). Then $s_h(t)$ can be

written as

$$\begin{aligned} & s_h(t) \\ &= \sum_{i\in I}[\sum_{v=0}^{k-1}(\alpha^{2t}+\gamma_h\alpha^{(2^{mk}+1)t}+ \\ &\qquad\qquad \alpha^{2^{mk+1}t})^{u2^{mv}}]^i \\ &= \sum_{i\in I}(\sum_{v=0}^{k-1}[x^2(1+\gamma_h y+y^2)]^{u\cdot 2^{mv}})^i \\ &= \sum_{i\in I}\prod_{j=1}^{w(i)}\sum_{v=0}^{k-1}[x^2(1+\gamma_h y+y^2)]^{u\cdot 2^{mv+i_j}} \\ &= \sum_{i\in I}\sum_{\underline{v}\in V^{w(i)}}[x^2(1+\gamma_h y+y^2)]^{\delta(i,\underline{v})} \end{aligned} \tag{13}$$

where $V=\{0,1,\cdots,k-1\}$, $\underline{v}=(v_1,v_2,\cdots,v_{w(i)})\in V^{w(i)}$, and

$$\delta(i,\underline{v})=\sum_{j=1}^{w(i)} u\cdot 2^{mv_j+i_j}. \tag{14}$$

We can now count the number of monomials in α^t with nonzero coefficients occurring in right side of Eq. (13), similar to the proof for Lemma 1 from [13].

Lemma 1: For different pairs $(i,\underline{v})$ and $(i',\underline{v'})$, there is no monomial that appears with nonzero coefficients in the expansions of both $(x^2(1+\gamma y+y^2))^{\delta(i,\underline{v})}$ and $(x^2(1+\gamma y+y^2))^{\delta(i',\underline{v'})}$.

Let $\rho(i,\underline{v})$ denote the number of monomials in y appearing in the expansion of $(1+\gamma_h y+y^2)^{\delta(i,\underline{v})}$ with nonzero coefficients. By Eq. (13) and Lemma 1, one has

$$LS(\{s_h(t)\})=\sum_{i\in I}\sum_{\underline{v}\in V^{w(i)}}\rho(i,\underline{v}). \tag{15}$$

Furthermore, Eq. (15) can be written as follows.

Proposition 1:

$$LS(\{s_h(t)\})=\sum_{i\in I\cap\Gamma(m)}\sum_{\underline{v}\in V^{w(i)}} e_i\cdot\rho(i,\underline{v}). \tag{16}$$

Proof: The index set I is a union of several cyclotomic cosets, i.e., $I=\cup_{i\in I\cap\Gamma(m)}C_i$. To prove Eq. (16), it is sufficient to show that

$$\sum_{\underline{v}\in V^{w(i)}}\rho(i,\underline{v})=\sum_{\underline{v}\in V^{w(i')}}\rho(i',\underline{v}) \tag{17}$$

holds for any $i,i'\in I$ with $i\equiv 2i' \bmod(2^m-1)$.

In Eq. (13), let

$$\begin{aligned} & \Delta(x) \\ &= \sum_{v=0}^{k-1}(x^2+\gamma_h x^{(2^{mk}+1)}+x^{2^{mk+1}})^{u2^{mv}} \\ &= tr_m^{mk}[(x^2(1+\gamma_h y+y^2))^u]. \end{aligned}$$

For any $x \in F_{2^n}$, $\Delta(x) \in F_{2^m}$ and hence $\Delta(x)^i = (\Delta(x)^{i'})^2$ if $i \equiv 2i' \bmod(2^m - 1)$. From Eq. (13), one has

$$\Delta(x)^i = \sum_{\underline{v} \in V^{w(i)}} [x^2(1 + \gamma_h y + y^2)]^{\delta(i,\underline{v})},$$

and then

$$\begin{aligned} &\sum_{\underline{v} \in V^{w(i)}} [x^2(1 + \gamma_h y + y^2)]^{\delta(i,\underline{v})} \\ &= \{ \sum_{\underline{v} \in V^{w(i')}} [x^2(1 + \gamma_h y + y^2)]^{\delta(i',\underline{v})} \}^2. \end{aligned}$$

Since $(\Delta(x)^{i'})^2$ and $\Delta(x)^{i'}$ have the same number of nonzero monomials in their expansions, comparing the numbers of nonzero monomials in the expansions of the both sides of the above equality, Eq. (17) holds.

By Proposition 1, the linear span can be determined by finding $\rho(i, \underline{v})$ for all $i \in I \cap \Gamma(m)$ and $\underline{v} \in V^{w(i)}$.

The number of nonzero monomials in the expansion of $(1 + \gamma_h y + y^2)^j$ is determined for $j < 2^{mk} - 1$ [12]. When $j \geq 2^{mk} - 1$, we can replace j with $j \bmod(2^{mk} - 1)$. Then, $\rho(i, \underline{v})$ equals to the number of nonzero monomials in the expansion of $(1+\gamma_h y+y^2)^{\delta'(i,\underline{v})}$, where $\delta'(i, \underline{v})$ is the remainder of $\delta(i, \underline{v})$ modulo $2^{mk} - 1$.

For $\gamma_h \neq 0$, define $\varepsilon_h = -1$ if the quadratic $y^2 + \gamma_h \cdot y + 1 = 0$ is reducible over $F_{2^{mk}}$, and $\varepsilon_h = 1$ otherwise. Let c_h be an integer with $0 \leq c_h \leq 2^{mk-1}$ such that

$$\delta_h = \begin{cases} \alpha^{c_h(2^{mk}+1)} & \text{if } \varepsilon_h = -1 \\ \alpha^{c_h(2^{mk}-1)} & \text{if } \varepsilon_h = 1 \end{cases} \tag{18}$$

is a root of $y^2 + \gamma_h \cdot y + 1 = 0$. Let $g_h = \gcd(c_h, 2^{mk} + \varepsilon_h)$. Then, $g_h < 2^{mk-1}$ [12].

Let $R(i, \underline{v})$ be the total number of 1-runs occurring within the binary expansion of $\delta'(i, \underline{v})$, and $L(i, \underline{v}, j)$ be the length of the j-th 1-run, $1 \leq j \leq R(i, \underline{v})$, with the runs being consecutively numbered from the least to the most significant bits. Then, $\delta'(i, \underline{v})$ can be written as

$$\delta'(i, \underline{v}) = \sum_{j=1}^{R(i,\underline{v})} 2^{d_j} \cdot (\sum_{l=0}^{L(i,\underline{v},j)} 2^l),$$

where d_j denotes the lowest exponent of 2 associated with the j-th 1-run.

By Theorem 2 in [12], the number of monomials with nonzero coefficients appearing in the expansion of $(1 + \gamma_h y + y^2)^{\delta'(i,\underline{v})}$ is then

$$\begin{aligned} &\rho(i, \underline{v}) \\ &= \prod_{j=1}^{R(i,\underline{v})} \{2^{L(i,\underline{v},j)+1} - 1 - 2\lfloor \tfrac{(2^{L(i,\underline{v},j)}-1)g_h}{2^{mk}+\varepsilon_h} \rfloor\}. \end{aligned} \tag{19}$$

When $\gamma_h = 0$, one has

$$\rho(i, \underline{v}) = 2^{\tau(i,\underline{v})} \tag{20}$$

where $\tau(i, \underline{v})$ is the weight of $\delta'(i, \underline{v})$. It was proved in [12] that $\rho(i, \underline{v})$ is always larger for $\gamma_h \neq 0$ than for $\gamma_h = 0$. Thus, the linear span of the ideal autocorrelation sequence $\{s_0(t)\}$ is always less than that of other sequences in the family $\mathcal{F}$.

A run in a binary sequence is a subsequence consisting of consecutive 0s or 1s, which is neither preceded nor succeeded [18]. Run length is the number of symbols in a run and can provide useful information to analyze the properties of the sequence. In order to measure the value of $\rho(i, \underline{v})$, run lengths related to Eq. (19) deserve further consideration. Let

$$u = 1 + 2^m + \cdots + 2^{(k-2)m} \qquad k \geq 2. \tag{21}$$

Then

$$\delta(i, \underline{v}) = \sum_{j=1}^{w(i)} u \cdot 2^{mv_j + i_j} = \sum_{j=1}^{w(i)} \sum_{l=0}^{k-2} 2^{m(v_j + l) + i_j}. \tag{22}$$

Lemma 2: Let $c_{j,l}$ be the remainder of $v_j + l$ modulo k for $1 \leq j \leq w(i)$ and $0 \leq l \leq k-2$. Then

$$\delta'(i, \underline{v}) = \sum_{j=1}^{w(i)} \sum_{l=0}^{k-2} 2^{mc_{j,l} + i_j}. \tag{23}$$

Proof: Since $2^{m(v_j+l)} \equiv 2^{mc_{j,l}} \bmod (2^{mk} - 1)$, $\delta(i, \underline{v}) \equiv \delta'(i, \underline{v}) \bmod (2^{mk} - 1)$.

For a fixed j, any two elements of $\{v_j + l \,|\, 0 \leq l \leq k-2\}$ are pairwise incongruent modulo k. Then $\{c_{j,l} \,|\, 0 \leq l \leq k-2\}$ are pairwise different and take values of $k, k-1, \cdots$, and 1 for a maximal summation. Hence

$$\begin{aligned} \sum_{j=1}^{w(i)} \sum_{l=0}^{k-2} 2^{mc_{j,l} + i_j} &= \sum_{j=1}^{w(i)} 2^{i_j} \sum_{l=0}^{k-2} 2^{mc_{j,l}} \\ &\leq \sum_{j=1}^{w(i)} 2^{i_j} \sum_{l=1}^{k-1} 2^{ml} \\ &\leq (2^m - 1) \cdot \tfrac{2^{mk} - 2^m}{2^m - 1} \\ &< 2^{mk} - 1. \end{aligned}$$

Since $\delta'(i, \underline{v})$ is the remainder of $\delta(i, \underline{v})$ modulo $2^{mk} - 1$, Eq. (23) holds.

From the proof of Lemma 2 and Eq. (23), the weight of $\delta'(i, \underline{v})$ can be written as

$$\tau(i, \underline{v}) = (k-1) \cdot w(i). \tag{24}$$

To guarantee the period of $\{s_h(t)\}$ reaching $2^n - 1$, the parameter u must be relatively prime to $2^{mk} - 1$. The following lemma gives such an integer.

Lemma 3: Let $k \geq 2$ and u be defined as Eq. (21). Then

$$\gcd(u,\, 2^{mk} - 1) = \gcd(k-1,\, 2^m - 1).$$

Proof: Since

$$2^{mk} - 1 - (2^{2m} - 2^m)(1 + 2^m + \cdots + 2^{(k-2)m}) = 2^m - 1$$

and

$$1 + 2^m + \cdots + 2^{(k-2)m} = k - 1 (\mathrm{mod}\, 2^m - 1),$$

one has

$$\gcd(u,\, 2^{mk} - 1) = \gcd(u,\, 2^m - 1) = \gcd(k - 1,\, 2^m - 1).$$

From this point on, we assume $\gcd(k - 1,\, 2^m - 1) = 1$. Then, $\gcd(u,\, 2^{mk} - 1) = 1$.

To simplify Eq. (19), we consider a subfamily of $\mathcal{F}$ as

$$\begin{aligned} \mathcal{F}' = \{\{s_0(t)\}, \{s_h(t)\} : h \neq 0, \\ g_h < \tfrac{2^{mk}+\varepsilon_h}{2^{m-1}+\varepsilon_h} \text{ and } 0 \leq c_h \leq 2^{mk-1}\}. \end{aligned} \tag{25}$$

We will derive a lower bound for linear spans of sequences in this subfamily. Let $\phi(t)$ be the Euler's phi function. The size of the subfamily $\mathcal{F}'$ is given in [13] as

$$|\mathcal{F}'| = (\sum_{\substack{t|2^{mk}+1 \\ t>2^{m-1}}} \phi(t) + \sum_{\substack{t|2^{mk}-1 \\ t>2^{m-1}}} \phi(t))/2 + 1. \tag{26}$$

For a sequence $\{s_h(t)\}$ in $\mathcal{F}'$ with $h \neq 0$, we have

$$\rho(i, \underline{v}) = \prod_{j=1}^{R(i,\underline{v})} \{2^{L(i,\underline{v},\, j)+1} - 1\} \tag{27}$$

for any $i \in I$ and $\underline{v} \in V^{w(i)}$. By analyzing run intervals for exponents, a lower bound on $\sum_{\underline{v} \in V^{w(i)}} \rho(i, \underline{v})$ for some i is estimated as follows.

For $1 \leq t \leq m - 1$, let $i^{(t)} = \sum_{j=1}^{t} 2^{j-1}$ with the weight t.

Lemma 4: Let $1 \leq t \leq m - 1$. Then

(1) For $\gamma_h = 0$,

$$\sum_{\underline{v} \in V^t} \rho(i^{(t)}, \underline{v}) = (2^{k-1}k)^t.$$

(2) For $\gamma_h \neq 0$,

$$\sum_{\underline{v} \in V^t} \rho(i^{(t)}, \underline{v}) > 3^{k-1}k((3k-1)2^{k-2})^{t-1}.$$

Proof: (1) The conclusion follows that for each $\underline{v} \in V^t$, $\rho(i^{(t)}, \underline{v}) = 2^{(k-1)t}$ by Eq. (20) and Eq. (24).

(2) Assume $\gamma_h \neq 0$. We then establish a lower bound on $\sum_{\underline{v}' \in V^{t+1}} \rho(i^{(t+1)}, \underline{v}') / \sum_{\underline{v} \in V^t} \rho(i^{(t)}, \underline{v})$ for $1 \leq t \leq m - 2$ and then deduce the conclusion.

For any $\underline{v} = (v_1, \cdots, v_t) \in V^t$ and $v_{t+1} \in V$, let $\underline{v}' = (v_1, \cdots, v_t, v_{t+1}) \in V^{t+1}$. By Eq. (22) and Eq. (23),

$$\delta(i^{(t)}, \underline{v}) = \sum_{j=1}^{t} \sum_{l=0}^{k-2} 2^{m(v_j+l)+j-1}$$

and

$$\delta'(i^{(t)}, \underline{v}) = \sum_{j=1}^{t} \sum_{l=0}^{k-2} 2^{mc_{j,l}+j-1}.$$

There are similar expressions for $\delta(i^{(t+1)}, \underline{v'})$ and $\delta'(i^{(t+1)}, \underline{v'})$. Define

$$\widetilde{\delta}(i^{(t)}, \underline{v}) = \sum_{j=1}^{t} \sum_{l=0}^{k-1} 2^{mc_{j,l}+j-1}.$$

For fixed integers d and j ($0 \leq d \leq k-1$ and $1 \leq j \leq t$), there exists a unique integer l with $0 \leq l \leq k-1$ such that $c_{j,l} = d$. This indicates that all run intervals of $\widetilde{\delta}(i^{(t)}, \underline{v})$ are

$$\begin{aligned} &[0, t-1], [m, m+t-1], \cdots, \\ &\qquad [m(k-1), m(k-1)+t-1]. \end{aligned} \tag{28}$$

Similarly, the run intervals of $\widetilde{\delta}(i^{(t+1)}, \underline{v'})$ are

$$[0, t], [m, m+t], \cdots, [m(k-1), m(k-1)+t].$$

By deleting all terms of the form $2^{mc_{j,k-1}+j-1}$ ($1 \leq j \leq t$) from the binary expansion of $\widetilde{\delta}(i^{(t)}, \underline{v})$, the binary expansion of $\delta'(i^{(t)}, \underline{v})$ is obtained. Thus, the run intervals of $\delta'(i^{(t)}, \underline{v})$ can be obtained by deleting the integers $mc_{j,k-1} + j - 1$ ($1 \leq j \leq t$) from the run intervals in Eq. (28).

The run interval of $\delta'(i^{(t)}, \underline{v})$ is called a type-I interval if it contains an integer of form $mc_{t,l} + t - 1$, where $0 \leq l \leq k-2$; otherwise, it is called a type-II interval. Thus, $\delta'(i^{(t)}, \underline{v})$ has exactly $(k-1)$ run intervals of type-I. Let u_l denote the length of the run interval containing $mc_{t,l} + t - 1$.

When $v_{t+1} = v_t$, for any $0 \leq l \leq k-1$, one has

$$v_{t+1} + l = v_t + l \text{ and } mc_{t+1,l} + t = (mc_{t,l} + t - 1) + 1.$$

This means that the length of each type-I run interval of $\delta'(i^{(t+1)}, \underline{v'})$ is larger by 1 than that of a corresponding type-I run interval of $\delta'(i^{(t)}, \underline{v})$, and that all type-II run intervals of $\delta'(i^{(t+1)}, \underline{v'})$ coincide with that of $\delta'(i^{(t)}, \underline{v})$. (Example 1 (1) illustrates this.) Thus,

$$\begin{aligned} \frac{\rho(i^{(t+1)}, \underline{v'})}{\rho(i^{(t)}, \underline{v})} &= \prod_{l=0}^{k-2} \frac{2^{u_l+1+1}-1}{2^{u_l+1}-1} \\ &> \prod_{l=0}^{k-2} 2 = 2^{k-1}. \end{aligned} \tag{29}$$

When $v_{t+1} \neq v_t$, one has

$$mc_{t+1,l'} + t = (mc_{t,l} + t - 1) + 1$$

if and only if

$$l' = l + v_t - v_{t+1} (\mathrm{mod}\, k). \tag{30}$$

Let l_0 $(0 \le l_0 \le k-1)$ be the unique solution of

$$l + v_t - v_{t+1} = k - 1 (\mathrm{mod}\, k). \tag{31}$$

Then $0 \le l_0 \le k-2$.

For any $0 \le l \le k-2$ with $l \ne l_0$, let $0 \le l' \le k-2$ be determined by Eq. (30). Then among the run intervals of $\delta'(i^{(t+1)}, \underline{v'})$, the length of the interval containing the integer $mc_{t+1,l'} + t$ is larger by 1 than that of the interval of $\delta'(i^{(t)}, \underline{v})$ containing $mc_{t,l} + t - 1$. On the other hand, the interval of $\delta'(i^{(t)}, \underline{v})$ containing the integer $mc_{t,l_0} + t - 1$ is identical to a corresponding interval of $\delta'(i^{(t+1)}, \underline{v'})$ and so does each type-II interval of $\delta'(i^{(t)}, \underline{v})$. Notice that the integer $mc_{t,k-1} + t$ is not in any interval of $\delta'(i^{(t)}, \underline{v})$, and $[mc_{t,k-1} + t] = [mc_{t+1,l_1} + t]$ is a single-point run interval of $\delta'(i^{(t+1)}, \underline{v'})$, where $l_1 = k - 1 + v_t - v_{t+1} (\mathrm{mod} k)$ and $0 \le l_1 \le k-2$. (Example 1 (2) illustrates this.) Thus,

$$\begin{array}{rcl} \frac{\rho(i^{(t+1)}, \underline{v'})}{\rho(i^{(t)}, \underline{v})} & = & (2^{1+1} - 1) \prod\limits_{l=0, l \ne l_0}^{k-2} \frac{2^{u_l+1+1} - 1}{2^{u_l+1} - 1} \\ & > & 3 \cdot 2^{k-2}. \end{array} \tag{32}$$

Applying Eq. (29) and Eq. (32), one has

$$\begin{array}{l} \sum\limits_{\underline{v'} \in V^{t+1}} \rho(i^{(t+1)}, \underline{v'}) \\ = \sum\limits_{\underline{v} \in V^t} \Big(\sum\limits_{v_{t+1} = v_t} \rho(i^{(t+1)}, (\underline{v}, v_{t+1})) \\ \qquad + \sum\limits_{v_{t+1} \ne v_t} \rho(i^{(t+1)}, (\underline{v}, v_{t+1})) \Big) \\ > \sum\limits_{\underline{v} \in V^t} (2^{k-1} + (k-1) 3 \cdot 2^{k-2}) \rho(i^{(t)}, \underline{v}) \\ = (3k-1) \cdot 2^{k-2} \sum\limits_{\underline{v} \in V^t} \rho(i^{(t)}, \underline{v}). \end{array} \tag{33}$$

For $v_1 \in V = \{0, 1, \cdots, k-1\}$, one has $\delta(1, v_1) = \sum\limits_{l=0}^{k-2} 2^{m(v_1 + l)}$ and $\delta'(1, v_1) = \sum\limits_{l=0}^{k-2} 2^{mc_{1,l}}$. There are exactly $(k-1)$ 1-runs of length 1. Thus,

$$\rho(i^{(1)}, v_1) = \rho(1, v_1) = \prod_{l=0}^{k-2} (2^{1+1} - 1) = 3^{k-1},$$

and

$$\sum_{v_1 \in V} \rho(1, v_1) = k \cdot 3^{k-1}. \tag{34}$$

Applying Eq. (34), and Eq. (33) iteratively, one has Lemma 4 (2).

Example 1: (1) Suppose that $m = 7$, $k = t = 4$, $\underline{v} = (3, 0, 3, 1)$ and $\underline{v'} = (3, 0, 3, 1, 1)$. The run intervals of $\widetilde{\delta}(i^{(5)}, \underline{v'})$ and $\widetilde{\delta}(i^{(4)}, \underline{v})$ are

$$[0, 3], [7, 10], [14, 17], [21, 24]$$

and

$$[0,4],[7,11],[14,18],[21,25],$$

respectively. A direct calculation will find the run intervals of $\delta(i^{(4)},\underline{v})$ and $\delta(i^{(5)},\underline{v'})$ are

$$[0,2],[7,10]^*,[15],[17]^*,[21],[23,24]^*$$

and

$$[0,2],[7,11]^*,[15],[17,18]^*,[21],[23,25]^*,$$

respectively, where the intervals marked with $*$ are in type-I and type-II otherwise.

Obviously, the type-I run intervals $[7,11],[17,18]$, and $[23,25]$ are of lengths larger by 1 than $[7,10],[17]$, and $[23,24]$, respectively, and all type-II run intervals of $\delta(i^{(5)},\underline{v'})$ and $\delta(i^{(4)},\underline{v})$ coincide.

(2) If $\underline{v'}=(3,0,3,1,2)$, then the run intervals of $\delta(i^{(5)},\underline{v'})$ are

$$[0,2],[4],[7,10]^+,[15],[17,18]^*,[21],[23,25]^*.$$

Since $l_0=k-1+v_{t+1}-v_t=0\,(\mathrm{mod}\,k)$, for $0\le l\le k-2$ with $l\ne l_0$, i.e., for $l=1$ or 2, $l'=l+v_t-v_{t+1}=0$ or 1. Then

$$\{mc_{t+1,l'}+t\,|\,l'=0,2\}=\{18,25\},$$

and we get two type-I run intervals marked with $*$, i.e., $[17,18]$ and $[23,25]$. Since $l_1=k-1+v_t-v_{t+1}=2(\mathrm{mod}\,k)$, the remaining type-I run interval is the single-point set [4]. The type-I interval of $\delta(i^{(4)},\underline{v})$ containing $mc_{t,l_0}+t-1=10$ is [7,10], it is a type-II interval of $\delta(i^{(5)},\underline{v'})$, which is marked with $+$. Other type-II run intervals of $\delta(i^{(5)},\underline{v'})$ and $\delta(i^{(4)},\underline{v})$ coincide.

Since $r=2^{m-1}-1\in I$, we have $i^{(m-1)}\in I\cap\Gamma(m)$. The size of the cyclotomic coset containing $i^{(m-1)}$ is m. Applying Proposition 1 to such an index set I gives

$$LS(\{s_h(t)\})\ge m\cdot\sum_{\underline{v}\in V^{m-1}}\rho(i^{(m-1)},\underline{v}). \tag{35}$$

Applying Lemma 4 to Eq. (33), one has the theorem below.

Theorem 1: Let $\{s_h(t)\}\in\mathcal{F}'$.

(1)

$$LS(\{s_0(t)\})\ge L_0=m(2^{k-1}k)^{m-1}.$$

(2) For $h\ne 0$,

$$LS(\{s_h(t)\})>L_1=3^{k-1}mk[2^{k-2}(3k-1)]^{m-2}.$$

Table 1 summarizes the family size and maximum linear span properties of some families with optimal correlation properties. In the small set of Kasami sequences, all sequences except the one with ideal autocorrelation property have the maximum linear

Table 1: Families of binary sequences of period $2^n - 1$ with optimal correlation $R_{\max} = 2^{\frac{n}{2}} + 1$.

Family	n	Family size	Maximum linear span
Bent function sequences	$4m$	$2^{\frac{n}{2}}$	$\geq \binom{n/2}{n/4} 2^{n/2}$
Kasami (small set)	$2m$	$2^{\frac{n}{2}}$	$\frac{3n}{2}$
No	$2m$	$2^{\frac{n}{2}}$	$n(2^{\frac{n}{2}} - 1)/2$
TN	$2mk$	$2^{\frac{n}{2}}$	$> 3n(3k-1)^{m-2}/2$
Sequences we studied	$2mk$	$2^{\frac{n}{2}}$	$> 3^{k-1}n[2^{k-2}(3k-1)]^{m-2}/2$

span $3n/2$ [6, 7]. The subfamily $\mathcal{F}' \setminus \{\{s_0(t)\}_{0 \leq t < 2^n - 1}\}$ consists of the sequences with maximum linear span in the proposed family $\mathcal{F}$. The size of $\mathcal{F}'$ is completely determined by the method proposed by Klapper [13]. This method in [13] is used to determine the subfamilies with maximum linear span respectively in No sequences and TN sequences. The subfamily sizes are listed as in Table 2. For a fixed value n and $k \geq 2$, by Table 2, one has

$$\begin{aligned} & \sum_{\substack{t|2^{mk}+1 \\ t>2^{m-1}}} \phi(t) + \sum_{\substack{t|2^{mk}-1 \\ t>2^{m-1}}} \phi(t) \\ = & \sum_{\substack{t|2^{n/2}+1 \\ t>2^{n/2k-1}}} \phi(t) + \sum_{\substack{t|2^{n/2}-1 \\ t>2^{n/2k-1}}} \phi(t) \\ > & \sum_{\substack{t|2^{n/2}+1 \\ t>2^{n/2-1}}} \phi(t) + \sum_{\substack{t|2^{n/2}-1 \\ t>2^{n/2-1}}} \phi(t). \end{aligned} \tag{36}$$

This shows that among all families in Table 2, the subfamily size of the small set of Kasami sequences is the largest and that of No sequences is the smallest. By a well-known fact

$$\sum_{t|d} \phi(t) = d, \ d > 0$$

from number theory, the cardinality of subfamily $\mathcal{F}' \setminus \{\{s_0(t)\}_{0 \leq t < 2^n - 1}\}$ can be measured. For $m, k \geq 2$,

$$\begin{aligned} & (\sum_{\substack{t|2^{mk}+1 \\ t>2^{m-1}}} \phi(t) + \sum_{\substack{t|2^{mk}-1 \\ t>2^{m-1}}} \phi(t))/2 \\ = & (2^{mk+1} - \sum_{\substack{t|2^{mk}+1 \\ t\leq 2^{m-1}}} \phi(t) - \sum_{\substack{t|2^{mk}-1 \\ t\leq 2^{m-1}}} \phi(t))/2 \\ > & 2^{mk} - 2^{m-1} \times 2^{m-1}/2 \\ = & 2^{mk} - 2^{2m-3}, \end{aligned} \tag{37}$$

Table 2: Family size of sequences with maximum linear span.

Family	n	Family Size
Kasami (Small set)	$2m$	$2^{\frac{n}{2}}-1$
No	$2m$	$(\sum_{\substack{t\mid 2^m+1\\ t>2^{m-1}}}\phi(t)+\sum_{\substack{t\mid 2^m-1\\ t>2^{m-1}}}\phi(t))/2$
TN	$2mk$	$(\sum_{\substack{t\mid 2^{mk}+1\\ t>2^{m-1}}}\phi(t)+\sum_{\substack{t\mid 2^{mk}-1\\ t>2^{m-1}}}\phi(t))/2$
The proposed family $\mathcal{F}$	$2mk$	$(\sum_{\substack{t\mid 2^{mk}+1\\ t>2^{m-1}}}\phi(t)+\sum_{\substack{t\mid 2^{mk}-1\\ t>2^{m-1}}}\phi(t))/2$

where the inequality holds since $\phi(t) < t$ and each factor of $2^{mk} \pm 1$ is odd. The formula

$$(2^{mk} - 2^{2m-3})/2^{mk} = 1 - 2^{(2-k)m-3} \geq 7/8 \tag{38}$$

shows that $\mathcal{F}'$ consists of a majority of sequences in the family $\mathcal{F}$ if $k \geq 2$.

The bounds for linear span of No sequences and TN sequences are $O(n \cdot 4^{\frac{n}{4}})$ and $O(n \cdot 5^{\frac{n}{4}})$, respectively [12], [13]. More precisely, let $U_N = 2^{\frac{n}{2}} \cdot n/2$ and $U_T = 9n \cdot (16/3)^{\frac{n}{4}-3}$. Then U_N and U_T are upper bounds on linear spans of No sequences and TN sequences.

For a large integer n, the lower bound L_1 given in Theorem 1 is maximized when $k = 4$. By Lemma 4, we choose $k = 4$ when m is odd and choose $k = 3$ or 5 when m is even. Table 3 lists the bounds L_0 and L_1, and the bounds $O(n \cdot 2^{\frac{2n}{3}})$, $O(n \cdot 44^{\frac{n}{8}})$ and $O(n \cdot 112^{\frac{n}{10}})$, which are exponentially larger than U_N and U_T, are given by taking $k = 3, 4, 5$, respectively.

4 An extension to sequences with ideal autocorrelation

This section tightens the bound in Theorem 1 and proves that a class of ideal autocorrelation sequences has large linear span. Most of the existing ideal autocorrelation sequences have very small linear span. Legendre sequences of a prime period can achieve an upper bound on linear span of binary ideal autocorrelation sequences [19].

Let $p = 2^m - 1$ be a Mersenne prime for some prime $m \geq 3$. A Legendre sequence of period p is defined as $\{a(t)\}$ where

$$a(t) = \begin{cases} 0, & \text{if } t \text{ is a quadratic residue modulo } p; \\ 1, & \text{otherwise.} \end{cases} \tag{39}$$

Table 3: The lower bound of linear span of sequences with period $2^n - 1$ in family $\mathcal{F}'$.

k	3	4	5
n	$6m$	$8m$	$10m$
L_0	$12^{\frac{n}{6}}n/72$	$2^{\frac{5n}{8}}n/256$	$80^{\frac{n}{10}}n/800$
L_1	$9n \cdot 2^{\frac{2n}{3}}/512$	$27n \cdot 44^{\frac{n}{8}}/3872$	$81n \cdot 112^{\frac{n}{10}}/25088$

The Legendre sequence has ideal autocorrelation. Below is its trace representation.

Lemma 5: ([20]) Let γ be a primitive element of Z_p. There is a primitive element β of F_{2^m} such that

$$a(t) = \sum_{j=0}^{\frac{p-1}{2m}-1} tr_1^m(\beta^{\gamma^{2j}t}) \tag{40}$$

is the trace representation of $\{a(t)\}$.

For $\zeta = 0$ or 1, define two sequences $\{a^{(\zeta)}(t)\}$ where

$$a^{(\zeta)}(t) = \sum_{j=0}^{\frac{p-1}{2m}-1} tr_1^m(\beta^{t\gamma^{2j+\zeta}}). \tag{41}$$

Then, $\{a^{(0)}(t)\} = \{a(t)\}$, and $\{a^{(1)}(t)\}$ is the γ-decimation of $\{a(t)\}$. Therefore, both sequences have ideal autocorrelation property.

Let $k \geq 2$ and $u = 1 + 2^m + \cdots + 2^{(k-2)m}$. Assume $\gcd(k-1, p) = 1$. We construct sequences of ideal autocorrelation from $\{a^{(0)}(t)\}$ and $\{a^{(1)}(t)\}$ as follows. For $\zeta = 0$ or 1, define

$$\begin{aligned} & s^{(\zeta)}(t) \\ &= \sum_{j=0}^{\frac{p-1}{2m}-1} tr_1^m(\{tr_m^{mk}[(tr_{mk}^n(\alpha^{2t}))^u]\}^{\gamma^{2j+\zeta}}). \end{aligned} \tag{42}$$

Then, $\{s^{\zeta}(t)\}$ is an ideal autocorrelation sequence of period $2^{2mk} - 1$ [11].

The following lemma is needed for a tighter bound on the linear span of $\{s^{(\zeta)}(t)\}$.

Lemma 6: (1) ([20]) When i varies from 0 to $\frac{p-1}{m} - 1$, γ^i runs through all the $\frac{p-1}{m}$ cyclotomic cosets of size m modulo p. For some integer j, $\gamma^{\frac{p-1}{m}} = 2^j$.

(2) Among $\frac{p-1}{m}$ cyclotomic cosets of size m modulo p, the number of cosets consisting of integers of weight i is $\binom{m}{i}/m$.

Theorem 2: For either $\zeta = 0$ or 1, the linear span of sequences defined as in Eq. (42) satisfies

$$\begin{aligned} & LS(\{s^{(\zeta)}(t)\}) \\ &\geq \tfrac{1}{2}[(1 + 2^{k-1}k)^m - 1 - (2^{k-1}k)^m]. \end{aligned} \tag{43}$$

Proof: For $\zeta = 0$ or 1, Proposition 1 together with Eq. (20) and Eq. (24) yields

$$LS(\{s^{(\zeta)}(t)\}) = \sum_{j=0}^{\frac{p-1}{2m}-1} m \cdot (2^{k-1}k)^{w(\gamma^{2j+\zeta})}. \tag{44}$$

Then

$$\begin{aligned}
&LS(\{s^{(0)}(t)\}) + LS(\{s^{(1)}(t)\}) \\
&= \sum_{j=0}^{\frac{p-1}{2m}-1} m \cdot [(2^{k-1}k)^{w(\gamma^{2j})} + (2^{k-1}k)^{w(\gamma^{2j+1})}] \\
&= \sum_{j=0}^{\frac{p-1}{m}-1} m \cdot (2^{k-1}k)^{w(\gamma^{j})} \\
&= \binom{m}{1} \cdot (2^{k-1}k) + \binom{m}{2} \cdot (2^{k-1}k)^2 + \\
&\qquad\qquad \cdots + \binom{m}{m-1} \cdot (2^{k-1}k)^{m-1} \\
&= (1 + 2^{k-1}k)^m - 1 - (2^{k-1}k)^m.
\end{aligned}$$

Thus, Theorem 2 holds.

Remark: An analysis to $L_0 = m(2^{k-1}k)^{m-1}$ shows that, for any given n, the bound L_0 is maximized only if $k \leq 6$. In this case, if $m \geq 2^k \cdot k + 1$, then the bound in Theorem 2 is tighter than that in Theorem 1. More precisely,

$$\begin{aligned}
&\tfrac{1}{2}[(1 + 2^{k-1} \cdot k)^m - 1 - (2^{k-1} \cdot k)^m] \\
&\geq m(2^{k-1} \cdot k)^{m-1}
\end{aligned} \tag{45}$$

holds for $k \leq 6$ and $m \geq 2^k k + 1$.

In Eq. (42), the parameter $k \geq 2$. However, one can take $k = 1$ and define

$$\widetilde{s}^{(\zeta)}(t) = \sum_{j=0}^{\frac{p-1}{2m}-1} tr_1^m([tr_m^{2m}(\alpha^{2t})]^{\gamma^{2j+\zeta}}) \tag{46}$$

where $\zeta \in \{0, 1\}$. One can get two ideal autocorrelation sequences of period $2^{2m} - 1$, and their linear span can be shown as

$$LS(\{\widetilde{s}^{(\zeta)}(t)\}) = \sum_{j=0}^{\frac{p-1}{2m}-1} m \cdot 2^{w(\gamma^{2j+\zeta})} \tag{47}$$

by Proposition 1 and Eq. (20). An analysis similar to Theorem 2 shows either $\{\widetilde{s}^{(0)}(t)\}$ or $\{\widetilde{s}^{(1)}(t)\}$ has linear span not less than $(3^m - 1 - 2^m)/2$.

Example 2: Let $\{a(t) = \sum_{j=0}^{8} tr_1^7(\alpha^{3^{2j}t})\}$ be a Legendre sequence of period 127 and $\{b(t) = a(3t)\}$ be its 3-decimation. The linear span of the sequence $\{s^{(1)}(t)\}$ derived from $\{b(t)\}$ is $1232 > 1029 = (3^7 - 1 - 2^7)/2$.

5 Conclusions

This paper finds a new sub-family of the generalized Kasami signal set in [11], which was defined by

$$\Gamma = \{g(tr^n_{n/2}(x^2) + \beta x^{2^{mk}+1}), \quad \beta \in F_{2^{mk}}, x \in F^*_{2^n}\}. \tag{48}$$

Here, $g(x) = tr^m_1\{[tr^{mk}_m(x^u)]^r\}$, $r = 2^{m-1}-1$, and $u = 1+2^m+\cdots+2^{(k-2)m}$. Generalized Kasami signal sets have optimal correlation property with respect to the Welch bound [16], and the linear span of sequences in Γ depends on $g(x)$. For suitable parameters, we prove that a majority of sequences in the family $\mathcal{F}$ in Eq. (2) can have linear spans exponentially larger than that of Kasami sequences (small set), No sequences and TN sequences. When implemented in future spread spectrum systems, the increased linear span of Generalized Kasami sequences can help to make it significantly harder for unauthorized terminals to synthesize spreading codes, and hence increase security of future spread spectrum systems.

6 Other Research Performed

The PI also studied free-space laser communications [21]-[24] and multiband radio transceivers with a shared RF frontend [25]-[27] during the funding period.

References

[1] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook.* McGraw Hill, 2001.

[2] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds., Amsterdam, The Netherlands: North-Holland, vol. II, pp. 1765-1853, 1998.

[3] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Trans. Inform. Theory*, vol. IT-13, no. 5, pp. 619-621, Oct. 1967.

[4] R. Gold, "Maximal recursive sequences with 3-valued recursive crosscrorlation functions," *IEEE Trans. Inform. Theory*, vol. IT-14, no. 1, pp. 154-156, Jan. 1968.

[5] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-function sequences" *IEEE Trans. Inform. Theory*, vol. IT-28, no. 6, pp. 858-864, Nov. 1982.

[6] T. Kasami, "Weight distribution formula for some class of cyclic codes," Coordinated Science Laboratory, University of illionos, Urbana, Tech. Rep. R-285 (AD632574), 1966.

[7] T. Kasami, "Weight distribution of Bose-Chaudhuri-Hocquenghem codes," in *Combinatorial Mathematics and Its Applications*. Chapel Hill, NC: Univ. North Carolina Press, 1969.

[8] X. Zeng, Q. Liu, and L. Hu, "A new family of codes and generalized Kasami sequences," in *2006 IEEE International Symposium on Information Theory*, pp. 907-911, 2006.

[9] X. Zeng, L. Hu, and W. Jiang, "A family of binary sequences with 4-valued optimal out-of-phase correlation and large linear span," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E89-A, No. 7, pp. 2029-2035, July 2006.

[10] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory,* vol. 15, no. 1, pp. 122-127, Jan. 1969.

[11] G. Gong, "New designs for signal sets with low cross correlation, balance property, and large linear span: GF(p) case," *IEEE Trans. Inform. Theory*, vol. 48, pp. 2847-2867, Nov. 2002.

[12] J. S. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," *IEEE Trans. Inform. Theory*, vol.35, no.2, pp. 371-379, March 1989.

[13] A. Klapper, "d-form sequences: families of sequences with low correlation values and large linear spans," *IEEE Trans. Inform. Theory*, vol. 41, no. 2, pp. 423-431, March 1995.

[14] R. Lidl and H. Niederreiter, *Finite fields. Encyclopedia of Mathematics and Its Applications*, vol. 20, Reading, MA: Addison-Wesley, 1983.

[15] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, Amsterdam, 1977.

[16] L. R. Welch, "Lower bounds on the mimimum correlation of signals," *IEEE Trans. Inform. Theory*, vol. 20, pp. 397-399, May 1974.

[17] E. L. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," *IEEE Trans. Inform. Theory*, vol. IT-22, no. 6, pp. 732-736, Nov. 1976.

[18] T. M. Cover and J. A. Thomas. *Elements of Information Theory.* Wiley, 1991.

[19] G. Gong and S. W. Golomb, "Binary sequences with two-level autocorrelation," *IEEE Trans. Inform. Theory*, vol. 45, no. 2, pp. 692-693, March 1999.

[20] J. S. No, H. K. Lee, H. Chung, H. Y. Song and K. Yang, "Trace representation of legendre sequences of mersenne prime period," *IEEE Trans. Inform. Theory*, vol. 42, no. 6, pp. 2254-2255, Nov. 1996.

[21] J. C. Brandenburg, and J. Q. Liu, "Optical signal detection in the turbulent atmosphere using p-i-n photodiodes," *IEEE J. Selected Areas in Commun.*, vol. 27, Dec. 2009.

[22] J. C. Brandenburg, and J. Q. Liu, "Signal detection for optical communications through the turbulent atmosphere," *IEEE Trans. Commun.*, vol. 57, pp. 3425-3432, Nov. 2009.

[23] J. Li, J. Q. Liu, and D. P. Taylor, "Optical communication using subcarrier PSK intensity modulation through turbulent atmospheric channel," *IEEE Trans. Commun.*, vol. 55, pp. 1598-1606, Jul. 2007.

[24] J. C. Brandenburg, and J. Q. Liu, "Signal detection in optical communications through the atmospheric turbulent channel," *Proc. IEEE Global Communications Conf.*, Nov. 30-Dec. 4, 2008, New Orleans, LA.

[25] S. Zakhem, and J. Q. Liu, "An approach for evaluating the performance of a multiband receiver with one sigma-delta ADC and one AGC," *Proc. IEEE Military Communications Conf.*, Oct. 18-21, 2009, Boston, MA.

[26] S. Zakhem, J. Q. Liu, and A. Macdonald, "Demodulation performance of multiband UWB communication system with one RF and ADC module receiver," *Proc. IEEE Military Communications Conf.*, Nov. 17-19, 2008, San Diego, CA.

[27] A. Macdonald, and J. Q. Liu, "The implications of 0.7 GHz to 3 GHz terrestrial band characterization on vehicular SDR design," *SDR Technical Conf.*, Oct. 26-30, 2008, Washington D.C.